JOURNAL OF ALGEBRA 123, 240–247 (1989)

On the Maximal p-Extensions of Real Quadratic Fields Unramified Outside p

KEIICHI KOMATSU

Department of Mathematics, Tokyo University of Agriculture and Technology, Fuchu, Tokyo, Japan

Communicated by A. Fröhlich

Received June 30, 1987

DEDICATED TO PROFESSOR TSUNEO KANNO ON HIS 60TH BIRTHDAY

INTRODUCTION

Let Q be the rational number field, p an odd number, and S a set of places of Q. Let $Q_S(p)$ be the maximal p-extension of Q unramified outside S and G the Galois group of $Q_S(p)$ over Q. Let (G, G) be the topological commutator group of G and $((G, G), G)$ the commutator group of (G, G) and G. Let H be the intermediate field of $Q_S(p)/Q$ such that the Galois group $G(Q_S(p)/H)$ is $((G, G), G)$. We call H the field of class two of $Q_S(p)/Q$ (cf. Fröhlich [3]). Fröhlich [3] determined the structure of $G(H/Q)$. This is a very deep result. In [7], using Galois cohomology, H. Koch obtained a generalization of Fröhlich's result. In the terminology of Koch, he treated only the "cases of known relations" (cf. [7]). In this paper, we treat a case of unknown relations. Namely, let k be a real quadratic field, ε the fundamental unit of k, h the class number of k, and L the maximal p-extension of k unramified outside p. We assume that p splits in k/Q and that p does not divide h. If $\varepsilon^{p-1} \equiv 1 \pmod{p^2}$, then $G(L/k)$ has an unknown relation. Let K be the field of class two of L/k. Let F be a free pro-p-group generated by x, y and let $\langle z \rangle_F$ be the minimal closed normal subgroup of F containing an element z of F. In this paper, using Iwasawa theory, we shall show the following:

If $\varepsilon^{p-1} \equiv 1 \pmod{p^2}$, then there exist p-adic integers α, β such that $G(K/k) \cong F/\langle x^{\alpha}(yxy^{-1}x^{-1})^{\beta} \rangle_F((F, F), F)$. Here, we can calculate α, β explicitly by calculating Stickelberger ideals (cf. Corollary of Theorem and Example).

Notations. We denote by Z the rational integer ring and Q by the rational number field. Let k be a finite algebraic extension of Q and v a

0021-8693/89 $3.00

place of k. We denote by $k^\times$ the multiplicative group of k and k_v the completion of k at v. For a prime number p, we denote by Z_p the p-adic integer rings and by $Z_p^\times$ the unit group of Z_p. Let G be a topological group and N a closed normal subgroup of G. We denote by G/N the factor group of G over N. For a subset S of G, we denote by $\langle S\rangle$ the closed subgroup of G generated by S and by $\langle S\rangle_F$ the minimal closed normal subgroup of G containing S. Let x, y be elements of G. We put $(x, y)=x^{-1}y^{-1}xy$. Let H, H' be closed subgroups of G. We denote by (H, H') the closed subgroup of G generated by a subset $\{(x, y)\mid x\in H, y\in H'\}$. For a finite algebraic extension L over k, we denote by $(L;k)$ the degree of L over k.

1. Galois Cohomology

Let p be an odd prime number, k a finite algebraic extension of Q, and S *a finite non-empty set of places of* k. We denote by $k_S(p)$ the maximal p-extension of k unramified outside S and by $G_S(p)$ the Galois group of $k_S(p)$ over k. We will use the abbreviation $H^i(G_S(p))$ for the cohomology groups $H^i(G_S(p), Z/pZ)$. It is well known that the number

$$m(G_S(p))=\dim_{Z/pZ} H^1(G_S(p))$$

coincides with the minimal number of generators of the pro-p-group $G_S(p)$. We call $m(G_S(p))$ the rank of $G_S(p)$. Let V_S be the following subgroup of k;

$$V_S=\{\alpha\in k^\times \mid \text{The principal ideal } (\alpha) \text{ is } p\text{-power of some ideal in } k \text{ and } \alpha\in k_v^p \text{ for } v\in S.\}$$

Let B_S be the dual of $V_S/(k^\times)^p$, r_1 the number of real places of k, and r_2 the number of imaginary places of k. Then we have

$$m(G_S(p))=\sum_{\substack{v\in S\\ v\mid p}}(k_v;Q_p)-\delta(k)-r_1-r_2+1+\sum_{v\in S}\delta(k_v)+\dim_{Z/pZ} B_S, \tag{1}$$

where $\delta(L)$, for a field L, is one if L contains a primitive pth root of 1 and zero otherwise (cf. Koch [6] and [7]). We know also that the number $r(G_S(p))=\dim_{Z/pZ} H^2(G_S(p))$ coincides with the minimal number of defining relations for $G_S(p)$. Shafarevich gave an estimate of $r(G_S(p))$:

$$r(G_S(p))\leqslant\sum_{v\in S}\delta(k_v)-\delta(k)+\dim_{Z/pZ} B_S \tag{2}$$

(cf. Koch [6] and [7]).

Let v be a place of S, $\tilde{k}_v$ the maximal p-extension of k_v, and $\tilde{G}_v$ the Galois group of $\tilde{k}_v$ over k_v. The noncanonical inclusion $k_S(p) \subset \tilde{k}_v$ induces a noncanonical mapping ϕ_v from $\tilde{G}_v$ into $G_S(p)$, which induces canonical mappings ϕ_v^* of the cohomology groups

$$H^i(G_S(p)) \xrightarrow[\phi_v^*]{} H^i(\tilde{G}_v).$$

Then we have a mapping

$$\phi_S^*: H^2(G_S(p)) \to \prod_{v \in S} H^2(\tilde{G}_v). \tag{3}$$

Let $U_S(p)$ be the kernel of ϕ_S^*. We call the number $u(G_S(p)) = \dim_{Z/pZ} U_S(p)$ the number of unknown relations of $G_S(p)$ in the terminology of Koch. In Koch [6], we see

$$\dim_{Z/pZ} U_S(p) \geqslant \dim_{Z/pZ} B_S. \tag{4}$$

2. Free Pro-p-Group of Rank 2

Let F be a free pro-p-group of rank 2 generated by $\{x, y\}$, $N = \langle x \rangle_F$ the minimal closed normal subgroup of F containing x, and $\Gamma = \langle y \rangle$ a closed subgroup of F generated by y. Then Γ is isomorphic to Z_p and F is a semi-direct product of Γ and N. We notice that N contains a topological commutator group (F, F) of F. Then we put $\Gamma^{p^n} = \langle y^{p^n} \rangle$, $\Gamma_n = \Gamma/\Gamma^{p^n}$, $F_n = \Gamma^{p^n} N$, $N_n \langle x, yxy^{-1}, \ldots, y^{p^n-1}xy^{-(p^n-1)} \rangle (F_n, F_n)$, and $X_n = N_n/(F_n, F_n)$. Since N_n contains N, Γ_n operates on X_n via inner automorphisms in the usual way. Namely, if $y^i \Gamma^{p^n} \in \Gamma_n$, we define

$$(y^i \Gamma^{p^n}) \circ t(F_n, F_n) = y^i t y^{-i}(F_n, F_n) \qquad \text{for all} \quad t(F_n, F_n) \in X_n.$$

Thus X_n is a Γ_n-module. Since $\{x, yxy^{-1}, \ldots, y^{p^n-1}xy^{-(p^n-1)}, y^{p^n}\}$ is a topological free generator system of F_n from Schreier's theorem, we can define a Γ_n-isomorphism f_n of X_n onto $Z_p[\Gamma_n]$ by $f_n(x(F_n, F_n)) = 1$. There are natural mappings $\phi_{m,n}: Z_p[\Gamma_m] \to Z_p[\Gamma_n]$ induced by the natural mapping $\Gamma_m \to \Gamma_n$ and $\psi_{m,n}: N_m/(F_m, F_m) \to N_n/(F_n, F_n)$ induced by the natural mapping $F_m/(F_m, F_m) \to F_n/(F_n, F_n)$ for $m \geqslant n$. Clearly we have $f_n \circ \psi_{m,n} = \phi_{m,n} \circ f_m$. The projective limit of the Γ_n-modules $N_n/(F_n, F_n)$ with respect to the mappings $\psi_{m,n}$ is $N/(N, N)$. Let $Z_p[[\Gamma]]$ be the projective limit of the group rings $Z_p[\Gamma_n]$ with respect to the mappings $\phi_{m,n}$. It is well known that there exists a topological isomorphism Φ of $Z_p[[\Gamma]]$ onto the ring $\Lambda = Z_p[[T]]$ of formal power series in an indeterminate T and Φ is induced by $\Phi(y) = 1 + T$ (cf. Coates [1]). Hence we can regard Λ

as Γ-module by $y \circ 1 = 1 + T$. Therefore we can define a Γ-isomorphism Ψ of $N/(N, N)$ onto Λ by $\Psi(x(N, N)) = 1$.

DEFINITION. A polynomial $P(T) \in Z_p[T]$ is called distinguished if $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ with $a_i \in pZ_p$ for $0 \leqslant i \leqslant n-1$.

Let G be a pro-p-group of rank 2 and of $\dim_{Z/pZ} H^2(G) = 1$. Then we may suppose that there exists an element r of N such that G is isomorphic to $F/\langle r \rangle_F$.

LEMMA 1. *Notations and assumptions being as above, if $r \notin (N, N)$, then there exist a positive integer d, a non-negative integer μ, p-adic integers $a_0, \ldots, a_{d-1}$ and an element r' of N such that*

$$\langle r' \rangle_F = \langle r \rangle_F, \qquad a_i \equiv \binom{d}{i} (-1)^{d-i} \pmod{p},$$

and

$$r' \equiv ((y^d x y^{-d})(y^{d-1} x y^{-(d-1)})^{a_{d-1}} \cdots (y^i x y^{-i})^{a_i} \cdots x^{a_0})^{p^\mu} \pmod{(N, N)}.$$

Proof. Let Ψ be as above. Since $\Psi(r(N, N))$ is an element in $Z_p[[T]]$, there exist from the p-adic Weierstrass preparation theorem a distinguished polynomial $P(T) = T^d + b_{d-1}T^{d-1} + \cdots + b_0$, a unit $u(T)$ of $Z_p[[T]]$, and a non-negative integer μ such that $\Psi(r(N, N)) = p^\mu P(T)\, u(T)$. We put $G(V) = P(V-1) = V^d + a_{d-1}V^{d-1} + \cdots + a_0$. Then, clearly, we have

$$a_i \equiv \binom{d}{i} (-1)^{d-i} \pmod{p} \qquad \text{for} \quad i = 0, \ldots, d-1.$$

Moreover, we can pick a representative r' of $\Psi^{-1}(p^\mu P(T))$ in N such that $\langle r' \rangle_F = \langle r \rangle_F$. Then we have

$$r' \equiv (y^d x y^{-d}(y^{d-1} x y^{-(d-1)})^{a_{d-1}} \cdots x^{a_0})^{p^\mu} \pmod{(N, N)}.$$

Remark. It is easy from Schreier's theorem to see that the set of ranks of F_n for $n = 1, 2, \ldots$ is not bounded. Hence the rank of N is infinite. Therefore, if $r \in (N, N)$, the rank of $N/\langle r \rangle_F$ is infinite.

3. REAL QUADRATIC FIELDS

Let ζ_p be a primitive pth root of 1 and k a totally real field of finite degree. We put $k' = k(\zeta_p)$. Let k_∞ and k'_∞ be cyclotomic Z_p-extensions of k and k', respectively. Met M and M' be the maximal abelian p-extensions of

k_∞ and k'_∞ unramified outside p, respectively. Since the degree $(k'; k)$ is prime to p, there exists an intermediate field L between M' and k_∞ such that $M' = Lk'$ and $k' \cap L = k$. We notice that the Galois group $G(k'/k)$ is isomorphic to $G(M'/L)$ in a natural way and that $G(M'/k)$ is a semi-direct product of $G(M'/k')$ and $G(M'/L)$. Let $\omega: G(M'/L) \to Z_p^\times$ be the character such that $\zeta_p^\sigma = \zeta_p^{\omega(\sigma)}$ for all $\sigma \in G(M'/L)$. Let δ be the order of $G(M/L)$. We define

$$\varepsilon_i = \frac{1}{\delta} \sum_{\sigma \in G(M'/L)} \omega^i(\sigma)\, \sigma^{-1} \in Z_p[G(M'/L)]$$

for $i = 0, 1, ..., \delta - 1$. We put $X = G(M'/k'_\infty)$. The group $G(M'/L)$ acts on X via inner automorphisms. Since X is a pro-p-group, we can consider X as a $Z_p[G(M'/L)]$-module. We put $X_i = \varepsilon_i X$ for $i = 0, 1, ..., \delta - 1$. Then we see that X coincides with the direct sum $\bigoplus_{i=0}^{\delta-1} X_i$. Now we put $Y = \bigoplus_{i=1}^{\delta-1} X_i$. Then we have the following:

LEMMA 2. *The Galois group $G(M'/k'M)$ coincides with Y.*

Proof. We put $H = G(M'/k_\infty)$. Since the topological commutator group (H, H) is $G(M'/k'M)$, it is sufficient to prove $(H, H) = Y$. Let g be a generator of the cyclic group $G(M'/L)$. Then we have

$$gxg^{-1}x^{-1} = x^{\omega^i(g)-1} \in (H, H) \qquad \text{for} \quad i = 1, ..., \delta - 1 \text{ and } x \in X_i.$$

Since p does not divide $\omega^i(g) - 1$ for $i = 1, ..., \delta - 1$, we have $X_i \subset (H, H)$ for $i = 1, ..., \delta - 1$. Hence we have $Y \subset (H, H)$. Since the factor group H/Y is commutative, we have $Y \supset (H, H)$. Hence we have $Y = (H, H)$.

Now, from Lemma 2, we have $G(M/k) \cong G(k'M/k') \cong G(k'_\infty/k')\, X_0$. Therefore $G(M/k_\infty)$ is isomorphic to X_0 as a $G(k_\infty/k)$-module. Let A'_∞ be the p-primary subgroup of the ideal class group of k'_∞. Then we can consider A'_∞ as a $G(k'_\infty/k)$-module in the usual way. From Coates [1], the dual of $\varepsilon_1 A'_\infty$ and X_0 are isomorphic as Z_p-modules. Then, from Iwasawa [5], we have the following;

LEMMA 3. *Notations and assumptions being as above, if the μ-invariant of k'_∞/k' is equal to zero, then $\dim_{Z/pZ} X_0/pX_0 = \dim_{Z/pZ} \varepsilon_1 A'_\infty/p\varepsilon_1 A'_\infty$ is finite.*

From now on, we assume that k is a real quadratic field such that p splits in k/Q. Then it follows from [2] that the μ-invariant of k'_∞/k' is equal to zero. Let ε be a fundamental unit of k. Furthermore we assume that p does not divide the class number of k and that $\varepsilon^{p-1} \equiv 1 \pmod{p^2 Z_p}$. Let S be the set of primes of k which lie above p. Since k_v does not contain

ζ_p for $v \in S$, we have $H^2(\tilde{G}_v) = 0$ from Koch [6]. Hence, from (3), we have $H^2(G_S(p)) \cong U_S(p)$. We have $\dim_{Z/pZ} B_S = 1$ from the definition of B_S and $\varepsilon^{p-1} \equiv 1 \pmod{p^2 Z_p}$. Hence it follows from (2) and (4) that $U_S(p) \cong Z/pZ$. This shows that $r(G_S(p))$ and the number of unknown relations of $G_S(p)$ are equal to one. We should note that k has a unique Z_p-extension. Now, we state our theorem.

THEOREM. *Let p be an odd prime number and k a real quadratic field such that p splits in k/Q. Let ε be a fundamental unit of k and S the set of primes of k which lie above p. We assume that p does not divide the class number of k and that $\varepsilon^{p-1} \equiv 1 \pmod{p^2 Z_p}$. Let $k_S(p)$ be the maximal p-extension of k unramified outside S. Let F be a free pro-o-group of rank 2 generated by $\{x, y\}$, N the closed minimal normal subgroup of F containing x. Then there exist a positive integer d, p-adic integers $a_0, \ldots, a_{d-1}$, and an element r of N such that*

$$G(k_S(p)/k) \cong F/\langle r \rangle_F,$$

$$r \equiv (y^d x y^{-d})(y^{d-1} x y^{-(d-1)})^{a_{d-1}} \cdots (y^i x y^{-i})^{a_i} \cdots x^{a_0} \pmod{(N, N)}$$

and

$$a_i \equiv \binom{d}{i} (-1)^{d-i} \pmod{p} \qquad \text{for} \quad i = 0, \ldots, d-1.$$

Proof. By (1) and the above considerations, we have $m(G_S(p)) = 2$ and $r(G_S(p)) = 1$. From Remark of Lemma 1 and Lemma 3, we see set there exists an element $r \in N$ such that $G(k_S(p)/k) \cong F/\langle r \rangle_F$ and $r \notin (N, N)$. We can show $r \notin (N, N)$ also from the fact that k has a unique Z_p-extension. Hence our theorem follows from Lemma 1 and [2].

Let γ be a generator of $G(k'_\infty/k')$, n a positive integer, and ω_n a primitive p^nth root of 1 such that $\omega_{n+1}^p = \omega_n$. Then there exists a p-adic integer u such that $u \equiv 1 \pmod{p Z_p}$ and that $\omega_n^\gamma = \omega_n^u$ for any positive integer n. Let $\zeta_p(s)$ be the p-adic zeta-function of k. Then there exists an element $g(T)$ in the quotient field of Λ such that $(1+T-u)\, g(T) \in \Lambda$ and that $g(u^s - 1) = \zeta_p(s)$ (cf. [1]). We put $f(T) = (1+T-u)\, g(T)$. Then we have $X_0 \cong \Lambda/(f(u(1+T)^{-1} - 1))$ from Iwasawa's main conjecture which is already proved in this case (cf. [8]). Let $P(T)$ be a distinguished polynomial and $U(T)$ be a unit of Λ such that $f(T) = P(T)\, U(T)$. Then we may assume that

$$P(T-1) = a_0 + a_1 T + \cdots + a_{d-1} T^{d-1} + T^d.$$

Here d and $a_0, \ldots, a_{d-1}$ are as in the Theorem. Using Stickelberger elements we can calculate the above d and also $a_0, \ldots, a_{d-1}$ (cf. [1]).

COROLLARY. *Notations and assumptions being as above, let K be the field of class two of $k_S(p)/k$* (cf. *Fröhlich* [3]). *Then $G(K/k)$ is isomorphic to*

$$F/\langle x^{1+\sum_{i=0}^{d-1} a_i}(yxy^{-1}x^{-1})^{d+\sum_{i=1}^{d-1} ia_i}\rangle_F((F,F),F).$$

Proof. We put $G=G(k_S(p)/k)$. From the definition of the field of class two, we have $G(K/k)\cong G/((G,G),G)\cong F/\langle r\rangle_F((F,F),F)$. We have

$$(uv,w)\equiv(u,w)(v,w) \qquad (\mathrm{mod}((F,F),F))$$

and

$$(u,vw)\equiv(u,v)(u,w) \qquad (\mathrm{mod}((F,F),F))$$

for $u,v,w\in F$. Hence, since N is generated by $\{y^ixy^{-i}\mid i\in Z\}$, $(N,N)\subset((F,F),F)$. From our theorem, we have

$$\begin{aligned} r &\equiv (y^dxy^{-d})(y^{d-1}xy^{-(d-1)})^{a_{d-1}}\cdots x^{a_0} \\ &\equiv x^{1+\sum_{i=0}^{d-1} a_i}(y^{-1},x^{-1})^{d+\sum_{i=1}^{d-1} ia_i} \quad (\mathrm{mod}((F,F),F)). \end{aligned}$$

Remark. Using Stickelberger elements, we can calculate the above d and also $a_0,\ldots,a_{d-1}$ from Iwasawa's main conjecture which is already proved in this case.

EXAMPLE. For $k=Q(\sqrt{103})$ and $p=3$, we obtain $d=2$, $a_0\equiv -5 \pmod{81}$, and $a_1\equiv 16 \pmod{81}$. Hence, in this case, we have $G(K/k)\cong F/\langle x^{\alpha}(yxy^{-1}x^{-1})^{\beta}\rangle((F,F),F)$ with $\alpha\equiv 12 \pmod{81}$ and $\beta\equiv 18 \pmod{81}$.

ACKNOWLEDGMENTS

The author expresses his hearty thanks to Professor T. Fukuda, Professor S. Iyanaga, and Professor T. Kanno.

V. U. Stephen and B. W. Stephen have recently obtained very interesting results on class two galois groups (cf. [9]).

REFERENCES

1. J. COATES, p-Adic L-functions and Iwasawa theory, *in* "Algebraic Number Fields" (Durham Symposium, 1975; A. Fröhlich, Ed.), pp. 269–353, Academic Press, New York/London, 1977.
2. B. FERRERO AND L. WASHINGTON, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395.
3. A. FRÖHLICH, On fields of class two, *Proc. London Math. Soc.* **4** (1954), 235–256.

4. A. FRÖHLICH, Central extensions, Galois groups, and ideal class groups of number fields, *in* "Contemporary Mathematics," Vol. 24, American Mathematical Society, Providence, RI, 1983.
5. K. IWASAWA, Riemann–Hurwitz formula and p-adic Galois representations for number fields, *Tôhoku Math. J.* **33** (1981), 263–288.
6. H. KOCH, "Galoissche Theorie der p-Erweiterungen," Springer-Verlag, Berlin/Heidelberg/New York, 1970.
7. H. KOCH, Fields of class two and Galois cohomology, *in* "Algebraic Number Fields" (Durham Symposium, 1975; A. Fröhlich, Ed.), pp. 609–622, Academic Press, New York/London, 1977.
8. B. MAZUR AND A. WILES, Class fields of abelian extensions of Q, *Invent. Math.* **76** (1984), 179–330.
9. V. U. STEPHEN AND B. W. STEPHEN, Generators and relations for certain class two Galois groups, *J. London Math. Soc.* **34** (1986), 235–244.